



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of)	MAIL STOP AF
Jean-Sebastien Coron)	
Application No.: 09/937,397)	Group Art Unit: 2135
Filed: April 1, 2002)	Examiner: NIRAV B. PATEL
For: COUNTERMEASURE METHOD IN)	Confirmation No.: 9400
AN ELECTRIC COMPONENT)	
IMPLEMENTING AN ELLIPTICAL)	
CURVE TYPE PUBLIC KEY)	
CRYPTOGRAPHY ALGORITHM)	

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Applicant requests review of the final rejection of claims 1-15 set forth in the Office Action dated April 18, 2006. No amendments are being filed with this request.

The request is being filed with a Notice of Appeal.

Background

The claimed subject matter is generally directed to public key cryptography that is based upon elliptical curves. More particularly, the claims recite a countermeasure that inhibits the ability of a hacker, or the like, to discover the private key of a user by observing multiple cryptographic operations that employ the key. Background information on public key cryptography based upon elliptical curves is set forth in the specification at pages 3-7, and the techniques for attacking this type of cryptographic operation are described at pages 7-11.

The claimed countermeasure protects against these types of attacks by introducing an element of randomness in at least one of the parameters that is employed during the cryptographic operation. In one embodiment of the countermeasure, a randomized value for the private key d is employed. In another embodiment, a randomized value is used for the calculation modulus p . In a third embodiment, at least one of the points P, Q on the curve that are used to calculate the keys is made random.

Double Patenting Rejection

Claims 1-15 stand finally rejected on the grounds of obviousness-type double patenting, in view of claims 1-7 of U.S. Patent No. 6,914,986. The rejection contends that the subject matter of independent claims 1, 6 and 11 of the present application is the same as those of the '986 patent, with the exception of the recitation of "determining a security parameter s ". The Action goes on to allege that it would have been obvious to determine a security parameter for the algorithm. One issue to be reviewed is whether the final Office Action establishes a prima facie case of obviousness that meets the criteria set forth in MPEP §2143.

As pointed out in Applicant's response filed February 28, 2006, MPEP §2143 states that a prima facie case of obviousness requires that there be a suggestion or motivation "in the references themselves" to modify a reference's teachings. The double patenting rejection is based upon a bald conclusion of obviousness, without any support therefor. Specifically, despite an express acknowledgement of a distinction between the claims of the pending application and those of the '986 patent, the Office Action does not cite any reference to show that this distinction was

even known in the prior art, let alone that it would be obvious to apply it to the claimed subject matter of the '986 patent. Hence, the rejection fails to identify any motivation to modify the reference that can be found in the prior art.

Another of the criteria for a prima facie case of obviousness is that the reference "must teach or suggest all of the claim limitations." In addition to the specific distinction identified in the Office Action, Applicant's previous response pointed out a number of features recited in claims 1, 6 and 11 of the present application that are different from the claimed elements of the '986 patent. See, in particular, the second and third complete paragraphs on page 2 of the Response filed February 28, 2006. The final Office Action fails to acknowledge these arguments, or otherwise identify where the identified features can be found in the claims of the '986 patent. Hence, it fails to meet this criteria as well.

MPEP §804 states "any analysis employed in an obviousness-type double patenting rejection parallels the guidelines for analysis of a 35 U.S.C. §103 obviousness determination." As set forth above, the final Office Action does not meet the requirements for a prima facie case of obviousness under 35 U.S.C. §103. As such, it fails to establish a proper case for the double patenting rejection.

Rejection Under 35 U.S.C. §103

Claims 1-15 stand finally rejected under 35 U.S.C. §103, on the grounds that they are considered to be unpatentable over the article by Jerome A. Solinas entitled "An Improved Algorithm for Arithmetic on a Family of Elliptic Curves", in view of the Curiger et al. patent (U.S. 6,064,740). This ground of rejection was traversed in the Response filed February 28, 2006. Rather than repeat the arguments herein, the

Reviewing Panel is referred to the Response, beginning with the paragraph that starts at the bottom of page 2.

In the response, Applicant identified a number of claimed features that are not apparent from the Solinas article. At the middle of page 3 of the response, Applicant explicitly requested that, if the rejection is not withdrawn, the Examiner identify where the Solinas article teaches three specific steps recited in claim 1. The final Office Action does not respond to this argument, and particularly does not indicate any attempt to identify where any of the noted features of the claim are disclosed in the Solinas reference.

Similar considerations apply to claims 6 and 11. On page 4 of the Response, Applicant identified specific recitations in these claims that are not found in the references. Again, there is no showing in the final Office Action where these claimed features can be found in the prior art.

Furthermore, the final Office Action groups claims 1, 6 and 11 under a single statement of rejection. In making the rejection, it only refers to the recitations of claim 1. The Office Action does not recognize that independent claims 6 and 11 recite steps that are different from those recited in claim 1. As such, even if, for the sake of argument, it were to be assumed that claim 1 is not patentable over the cited references, the Office Action does not contain any showing that would justify the rejection of independent claims 6 and 11.

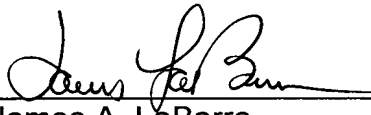
For at least the foregoing reasons, the final Office Action fails to establish a prima facie case of obviousness, for either of the grounds of rejection set forth therein. The double patenting rejection is based upon an unsupported conclusion of obviousness, and does not identify where a number of elements of the currently

pending claims are found in the claims of the '986 patent. The rejection under 35 U.S.C. §103 fails to show where a number of the features recited in the claims can be found in the references, despite Applicant's explicit request for such a showing.

There is an insufficient record to be presented to the Board of Patent Appeals and Interferences. Withdrawal of the final Office Action is respectfully submitted to be in order.

Respectfully submitted,
BUCHANAN INGERSOLL & ROONEY PC

Date: August 18, 2006

By: 
James A. LaBarre
Registration No. 28632

P.O. Box 1404
Alexandria, VA 22313-1404
703 836 6620